Remarks

Claims 52-58 have been canceled, and claims 1-51, 59-69, 73 and 74 are pending.

As an initial matter, the Examiner's extensive consideration and comments on the specification and claims was greatly appreciated.

Objections

The Examiner objected to the use of the same reference numbers to represent value notes that included different information in the various figures. The specification has been amended, and the Examiner's approval of corresponding changes to the reference numbers in the drawings (shown in red on the attached drawing sheets) is respectfully requested.

In particular, in Figure 6 reference number "20" is changed to "21", in Figure 9 reference number "50" is changed to "50b", in Figure 10 reference number "60" is changed to "60s", in Figure 11 reference number "20" is changed to "67", in Figure 12 reference number "20" is changed to "99", in Figure 13 reference number "50 (100)" is changed to "101), in Figure 14 reference number "20" is changed to "103", and in Figure 17 reference number "110" is changed to "111".

The Examiner also objected to the specification for various informalities. The specification has been amended, and in the main the Examiner's recommendations have been adopted as shown in the rewritten paragraphs.

Withdrawal of the rejections is requested, and the Examiner is encouraged to telephone the undersigned to resolve any remaining issues..

Rejections under 35 U.S.C. §112

Claims 1-48, 51, 65-69, 73 and 74 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

The claims have been amended to obviate the rejections, to provide antecedent basis, to correct typographical errors (such as the transposition of "redemption" and "instruction" in claim 28), and generally to clarify the meaning of the claim language (such as the use of the term "and/or" in claim 35).

Specifically, claim 1 was amended to clarify that the public key for the bearer/issuer is the bearer's/issuer's public key, respectively. This language was amended in the same manner throughout the claims.

The undersigned also notes that the specification clearly specifies that "[t]he invention uses digital signatures, which are calculated by a signatory when 'signing' or endorsing the value note." (Specification, p. 4, lines 14-15; the Examiner's attention also is directed to the rest of that paragraph at lines 14-25.) It is respectfully submitted that a person of ordinary skill in the art would understand "calculating information representative of a signature."

Claim 15 was amended to include the limitations of claim 1, from which it depended.

Claims 18 and 40 were amended as suggested by the Examiner, replacing "proportion" with "portion." However, these terms are substantially interchangeable and a person of ordinary skill in the art would have understood the meaning; no change is believed to be necessary.

Finally, claim 74 was amended to include physical elements for carrying out the method steps of claim 1.

Withdrawal of the rejections is requested.

Rejections under 35 U.S.C. §102/103

Claims 1, 3-52, 59-69, 73 and 74 have been rejected under 35 U.S.C. §102(e) or §103 as being unpatentable over U.S. Patent No. 5,889,862 to Ohta, et al. ("Ohta"), and/or further in view of U.S. Patent No. 5,224,162 to Okamoto, et al. ("Okamoto") or further in view of U.S. Patent No. 5,511,121 to Yacobi ("Yacobi").

With regard to Ohta, the Examiner has taken the position that (1) the public information N, corresponding to a user's real name ID_U, reads on the claimed first information representative of a bearer's public key information; (2) the electronic cash C reads on the second information representative of a commodity; and (3) the first institution's signature, represented by license B, reads on the claimed third information representative of an issuer's signature. In support, the Examiner cites Ohta column 23 lines 56-60 (steps 3 and 4 in claim 1 of Ohta).

In a review of the passage cited by the Examiner, and Ohta in general, no disclosure has been found of the claimed step (3) of calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by an issuer's public key information. If the license B is representative of the first institution's signature, the license B is not calculated based on the electronic cash C (see Ohta, col. 8, lines 33-67). Accordingly, the claimed invention is not believed to be anticipated by Ohta.

Furthermore, no teaching or suggestion has been found to motivate a person of ordinary skill in the art to modify the system described in the Ohta reference to derive the claimed invention. Ohta appears to describe a method whereby a bank issues a license B to use electronic cash C. Processing the license is described in Ohta, col. 8, line 33 through col. 9, line 23. The bank issues electronic cash based on a separate request from the user. See Ohta, col. 9, line 23 through col. 10, line 16. The payment of electronic cash and settlement with the shop owner (the payee) is described in Ohta, col. 10, line 17 through col. 11, line 27. Unlike the value note provided by the claimed invention, the license B does not have a value associated with it. Ohta's system is designed so that the electronic cash and the right to use it (the license B) are issued separately, therefore adding a commodity value to Ohta's license would destroy its intended purpose. Accordingly, a person of ordinary skill in the art would not have been motivated to derive the claimed invention upon reading and understanding Ohta.

In addition, the electronic cash described by Ohta does not include expiration information (see col. 10, line 17 through col. 11, line 27). In fact, since each item of electronic cash is fashioned as a numeric solution to a single calculation, adding date information could destroy required properties of the electronic cash. The passages cited by the Examiner in Ohta appear to describe providing information concerning when the license B is going to expire rather than when electronic cash C would expire. See claim 3, for example.

Furthermore, no disclosure has been found in Ohta of identification information associated with the electronic cash C or the license B. The passage cited by the Examiner refers to the process for obtaining a license B and does not provide unique identification for either the license B or a discrete item of electronic cash C. As noted above, no specified commodity value is associated with the license B. See claim 5, for example. The ability to provide unique identifying information for a value note allows the value note to be serially indexable – an advantage not provided by the system described in Ohta.

Consequently, these particular features cited in the dependent claims also have not been found in the Ohta reference.

The secondary references to Okamoto and Yacobi do not overcome the deficiencies of Ohta. It is further submitted that the claimed invention would not have been obvious in view of the applied references, that a person of ordinary skill in the art would not have combined Yacobi with Ohta because Yacobi and even if the combination was made the claimed invention would not result.

Withdrawal of the rejections is respectfully requested.

Conclusion

In view of the foregoing, the present application is believed to be in a condition for allowance and an early indication to that effect is earnestly solicited. **If the**

application is not believed to be in condition for allowance, the Examiner is asked to telephone the undersigned to resolve any remaining issues.

Should a petition for an Extension of Time be necessary for the timely reply to the outstanding Office Action (or if such a petition has been made and an additional extension is necessary) petition is hereby made and the Commissioner is authorized to charge any fees (including additional claim fees) to Deposit Account No. 18-0988, under Attorney Docket No. DYOUP0185US.

Respectfully submitted,

RENNER, OTTO, BOISSELLE & SKLAR, L.L.P.

Christopher B. Jacobs
Reg. No. 37,853

1621 Euclid Avenue
Nineteenth Floor
Cleveland, Ohio 44115
(216) 621-1113

CERTIFICATE OF MAILING (37 CFR 1.8a)

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, U.S. Patent and Trademark Office, Washington, D.C. 20231.

June 11, 2002
Date

Christopher B. Jacobs

K:\152\DWB\DYOU\P\P0185\P0185US.R02 Final.wpd

Appendix -- Amendment Version with Markings to Show Changes Made

The following is a marked-up version of the above amendments to the claims. Added material is underlined, and removed material struck out and in brackets.

In the Specification:
Please rewrite the paragraph on page 2, lines 23-24 as shown:

> OFF-LINE PAYMENT - To enable the electronic money to be transferred without needing to simultaneously contact [~~with~~] the bank at the time of transfer.

Please rewrite the paragraph on page 2, lines 26-32 as shown:

> NON-LIABILITY - Particularly when communicating over a public communication system, there are occasions when communication is interrupted, or a message is not confirmed as having been received, or a computer system crashes. In such a situation, it may be impossible to establish whether an instructed electronic money transaction or transfer has taken place. In other situations, data representing the electronic money might be lost. It is desirable that an electronic money user [~~to~~] be able to repeat the same transaction, or make "back-up" copies of the electronic money, without increasing the liability of the user and the bank.

Please rewrite the paragraph on page 9, lines 24-30 as shown:

> Such a technique achieves complete security for the new bearer even though the new value note will be handled by the original bearer. The new bearer will be able to verify the authenticity of the new value note

independently by means of the value note issuer's signature. Furthermore, it will be impossible for the original bearer to attempt to forge the new bearer's signature because the original bearer will only be aware of the new bearer's public key; the original bearer will not be aware of the new bearer's secret key which is required for writing an endorsement signature.

Please rewrite the paragraph on page 24, lines 18-31 as shown:

The next step (step 76 in Fig. 7) is for the buyer to append payment instruction information 68 to the value note 20 (Fig. 2), to form new value note 21 as illustrated in Fig. 6. In the present example, the payment instruction information instructs the bank to split the money value of the original value note 20 (Fig. 2) between the new value note 50 for the seller, and the new value note 60 for the buyer. The payment instruction information can identify each of the new value notes 50 and 60 by means of the bearer's reference 56 and 66, respectively. Also in this example, the respective currency values have been included in the seller's new value note 50, the buyer's new value note 60, as well as in the payment instruction information 68. This redundancy may be useful to ensure that no errors or mistakes occur in the new value note and the payment instruction information. However, the information might instead be included only once, either in the payment instruction information 68, the buyer's new value note 60, or the seller's new value note 50. For example, the bank computer 10 would be able to calculate the necessary "change" from the original value information 24 and the payment value 54 from the seller's new value note 50.

Please rewrite the paragraph on page 25, lines 15-32 as shown:

Having "signed" the value note [~~20~~] 21, the buyer would then transmit the endorsed value note [~~20~~] 21, the blank new buyer's value note 60 and the blank new seller's value note 50 through the communication network 14 to the bank computer 10 (step 78 in Fig. 7). The endorsed value note, and the blank value notes, may either be transmitted in their entirety or, alternatively, only selected information might be transmitted. For example, since each value note has its own unique identification number, the entire information in the value note does not itself need to be transmitted back to the issuing authority (the issuing authority will be able to access such information from their record copy of the original value note and, indeed, would normally access this information to verify the redemption instructions). In its briefest form, the instructions may be transmitted without any information from the original value note apart from the identification number. The instructions may also simply include a reference number and public key for each new value note to be generated (instead of transmitting a whole blank value note). An instruction format using such "reduced" information is described in more detail later; the current description is to be interpreted to cover using such "reduced" or short-hand information as well as transmitting full information. It is emphasised that the use of "reduced" information does not limit the information which can be included in the endorsing signature, since this can be based on all of the value information (such information being available to both the bearer and the money handling authority).

Please rewrite the paragraph on page 26, lines 1-5 as shown:

Referring to Fig. 8, the bank computer performs a number of verification tests upon the endorsed value note [~~20~~] 21 (Fig. 6) to determine its authenticity. The order in which the tests are performed is not important; if any one of the tests fails, then the bank computer 10 may treat the value note as being "false", and need not honour the value note.

Please rewrite the paragraph on page 26, lines 7-10 as shown:

In this example, the bank computer 10 first performs a test 80 upon the "valid from" date information 34 and the expiry date information 36 in the received original value note 20 (Fig. 2), (or in the copy of the note already held by the bank computer if the original note is not returned) to ascertain whether the current date falls within an allowable window.

Please rewrite the paragraph on page 26, lines 12-18 as shown:

Assuming that the date is satisfactory, the bank computer 10 next proceeds to step 82 at which the buyer's signature 70 is analysed. By using the public key information 22 originally presented in the value note 20 (Fig. 2), the bank computer 10 attempts to verify that the signature information 70 matches the information in the endorsed value note [~~20~~] 21 upon which the signature information 70 is based. As explained above, the signature information 70 depends at least upon the payment instruction information 68, and may also depend on other predetermined information in the value note.

Please rewrite the paragraph on page 26, line 27 through page 27, line 4 as shown:

At step 92 (in Fig. 8), the bank computer 10 completes the endorsed original value note [~~20~~] 21 to provide a receipt of the transaction to the buyer. The completed original value note [~~20~~] 67 is illustrated in Fig. 11. This includes an "OK" message indicated at 94, and a final bank signature 96. The final bank signature is calculated based on the text of the buyer's signature 70 described above, and acts as a guarantee that the buyer's signature cannot subsequently be altered, either by the bank or by the buyer, should a dispute arise later. As indicated in Fig. 11, the final bank signature 96 may also be based on other information in the value note [~~20~~] 67, such as the "valid from" information 32 (Fig. 2), the payment instruction information 68 (Fig. 6), and the "OK" message 94, to prevent alteration of those items of information in case of a dispute later.

Please rewrite the paragraph on page 27, lines 6-12 as shown:

If the above tests 80, 82 and 84 are all satisfied, this is indicative that the completed original value note [~~20~~] 67 has not been tampered with, and that the buyer is the correct bearer authorised to redeem the value note. The next test 86 performed by the bank computer 10 ascertains whether the value note [~~20~~] 67 has previously been redeemed. This test can be performed by comparing the bank's reference code 30 (Fig. 2) in the completed original value note [~~20~~] 67 with a list maintained in the bank computer 10 of each value note and the date, if any, of redemption. The purpose of this test 86 is to prevent a user from "double spending" a value note.

Please rewrite the paragraph on page 27, lines 14-20 as shown:

Assuming that the value note [~~20~~] 67 has not previously been redeemed, the bank computer records the current date as the date of redemption, and proceeds to step 88 at which the new seller's value note 50 is completed and a bank's signature added to authenticate the new value note 50 in the same manner as that described above for the value note 20. The completed seller's value note is illustrated in Fig. 9. This is similar to the original form of value note 20 shown in Fig. 2, and the same reference numerals (followed by the letter "s") are used to indicate the corresponding information in the completed value note [~~50~~] 50s.

Please rewrite the paragraph on page 27, lines 22-25 as shown:

Similarly, at step 90 (in Fig. 8), the new buyer's value note 60 is completed and a bank's signature is added to authenticate the new buyer's value note 60. The completed new buyer's value note [~~60~~] 60b is illustrated in Fig. 10, and corresponding reference numerals (followed by the letter "b") denote the value note information described previously.

Please rewrite the paragraph on page 27, line 27 through page 28, line 3 as shown:

At step 92 (in Fig. 8), the bank computer 10 completes the original value note 20 to provide a receipt of the transaction to the buyer. The completed original value note [~~20~~] 67 is illustrated in Fig. 11. This includes an "OK" message indicated at 94, and a final bank signature 96. The final bank signature is calculated based on the text of the buyer's signature 70 described above, and acts as a guarantee that the buyer's

signature cannot subsequently be altered, either by the bank or by the buyer, should a dispute arise later. As indicated in Fig. 11, the final bank signature 96 may also be based on other information in the value note [~~20~~] 67, such as the "valid from" information 32 (Fig. 2), the payment instruction information 68 (Fig. 6), and the "OK" message 94, to prevent alteration of those items of information in case of a dispute later.

Please rewrite the paragraph on page 28, lines 5-12 as shown.

Finally, at step 98 (in Fig. 8), the bank computer 10 transmits the new seller's value note [~~50~~] 50s, the new buyer's new value note [~~60~~] 60b and the completed original value note [~~20~~] 67 to the buyer's computer terminal. This is the computer terminal from which the original transaction instructions were transmitted to the bank computer 10. Upon receipt of the new value notes, the buyer would keep his own new value note [~~60~~] 60b for further use, and forward the new seller's value note [~~50~~] 50s to the seller as payment. The buyer's computer terminal would typically communicate with the seller's computer terminal through the public communication system 14 to transfer the seller's value note [~~50~~] 50s.

Please rewrite the paragraph on page 29, lines 1-8 as shown:

Any value note can be copied or distributed without increasing the liability of the bank, since the bank only has to honour the first valid presentation of a value note endorsed with payment instructions and a correct signature. The bank cannot avoid honouring at least one presentation, since it will not be able to demonstrate any other payment instructions except those correctly endorsed with the bearer's signature. If

the bank is queried over the disposal of any issued note, the bank will be able to issue confirmation copies of the receipt value note [~~20~~] 67 (Fig. 11), the seller's value note [~~50~~] 50s (Fig. 9) and the buyer's replacement value note [~~60~~] 60b (Fig. 10) without increasing its liability.

Please rewrite the paragraph on page 30, lines 19-27 as shown:

In the above, the "valid from" information in the new value notes [~~50~~] 50s and [~~60~~] 60b may simply represent the instantaneous date and/or time of issuance, as a record of the date and/or time of issuance. Alternatively, the "valid from" information of one or both of the new value notes [~~50~~] 50s and [~~60~~] 60b may be set a predetermined interval after the time and/or date of issuance. This is equivalent to "post-dating" the value note so that it cannot be used again for immediate redemption. A possible advantage of this is that it can prevent a malicious user from repeatedly submitting new value notes for redemption immediately after issuance, and thereby try to overload the bank's computers. The interval may, for example, be from a few minutes, or less, to a day, or longer, as desired.

Please rewrite the paragraph on page 31, lines 8-14 as shown:

Referring to Fig. 12, the buyer appends payment instruction information 100 to the endorsed original value note [~~20~~] 67 (Fig. 11), in a similar manner to that described previously. However, the payment instruction information 98 instructs the bank computer 10 to create a only temporary value note 99 (i.e. an option note) having a limited life. The payment instruction information further includes a delayed instruction that,

if the option note is not redeemed by the seller by an expiry date selected by the buyer, then the bank computer is to return the funds by issuing a second value note to the buyer.

Please rewrite the paragraph on page 31, lines 19-32 as shown:

Before the buyer sends the endorsed value note [~~20~~] 67 and the new blank value notes to the bank, the buyer appends further information to the seller's blank value note [~~50~~] 50s (Fig. 9) to transform it into a blank "option" note [~~100~~] 101. Referring to Fig. 13, the buyer adds option note information 102 about any further conditions or requirements which the seller must meet before the option note can be redeemed by the seller. Examples of such conditions are described below. The buyer may also include the expiry date information 104 for the option note (although these could also be included by the bank computer 10 (Fig. 1) later if desired). Finally, the buyer calculates a signature 106 based at least on the option note information 102 to endorse the option note information and prevent this from being altered later. As indicated in Fig. 13, the signature 106 may also be based on other information in the option note 101, such as the seller's public key 52, the value 54 of the option note, and the expiry date 104, to protect these other items of information. As explained previously, a reduced set of information may be used, consisting mainly of the redemption instructions, instead of returning a complete value note.

Please rewrite the paragraph on page 32, lines 1-3 as shown:

The buyer then transmits the modified seller's value note (i.e. the blank option note 101 in Fig. 13) with the endorsed value note [~~20~~] 67 and the buyer's two blank value notes, to the bank computer 10 (Fig. 1).

Please rewrite the paragraph on page 32, lines 5-8 as shown:

Fig. 14 illustrates the completed value note [~~20~~] 103 which the bank computer 10 (Fig. 1) returns to the buyer. This is similar to that shown in Fig. 11, and includes an "OK" message 94, and a final bank signature 96 to "sign off" the value note [~~20~~] 103.

Please rewrite the paragraph on page 33, lines 6-12 as shown:

Fig. 17 illustrates an endorsed option note [~~110~~] 111 which includes both of the above examples of option note information. The value note includes a signature 112 calculated by the seller to endorse the option note information 102, or at least a receipt string part of the option note information. In this embodiment, the receipt string comprises encrypted text so that neither the bank computer 10 nor bank staff can read the receipt text. This provides absolute anonymity for the transaction at the same time as providing a receipt decipherable by the buyer and seller.

Please rewrite the paragraph on page 34, lines 1-5 as shown:

When the blinded message T, the signature S and the [~~accompany~~] accompanying information M' and F are sent to the bank computer, the

bank computer can verify that the signature is valid by verifying that S = (M' ^ F) mod N. In this manner, the bank can verify that the seller has signed the message to the buyer, even though the bank is not able directly to read the blinded message T.

Please rewrite the paragraph on page 34, lines 16-20 as shown:

The endorsed option note also includes a second signature 114 calculated by the buyer, to meet the requirement in the option note information 102. The buyer's second signature should be calculated using text information [~~in~~] if the option note different is from that protected already by the buyer's endorsing signature 106. In this embodiment, the buyer's second signature is based on text comprising the bank's issuing signature 26.

Please rewrite the paragraph on page 35, lines 10-14 as shown:

After step 122, the bank computer proceeds to step 124 at which bank computer 10 tests whether the option note conditions include a requirement for the seller to endorse a text message (for example, an encrypted receipt message) with the seller's signature. If not, the routine branches past step 126 to indicate that the option note conditions have been met. If a seller's signature is required, step 126 tests whether it matches the receipt text provided by the buyer.

Please rewrite the paragraph on page 35, lines 20-26 as shown:

After the expiry date of the option note, the buyer may contact the bank computer 10 to enquire about the option note. For example, the buyer may submit a copy of the option note as evidence of [~~authorisation~~] authorization. If the seller has not redeemed the option note, the bank computer 10 can issue the new value note to the buyer at that stage to return the funds. On the other hand, if the seller has redeemed the option note, then the bank computer can provide a copy of the fully signed option note (Fig. 17) to the original buyer as a receipt for the transaction (which includes the receipt information presented in the option note information 102).

Please rewrite the paragraph on page 36, lines 10-18 as shown:

A further advantage is that if the buyer prepares one or more option notes in advance of potential transactions, the transactions can be performed "off-line" from the bank computer. The buyer may, for example, print [~~the or~~] each of the one or more option [~~note~~] notes on paper, and send or hand the option note to the seller. The seller will then have a certain period (for example, a few days) to make contact with the bank computer to redeem the option note (which is guaranteed up to that time). However, if for any reason the buyer decides not to proceed with any of the transactions and keeps the option notes for those transactions, the bank will simply return the funds to the buyer by issuing new value notes when the option notes expire. In this case, the seller never obtains the option notes.

Please rewrite the paragraph on page 37, lines 4-8 as shown:

Another application for option notes is for a secure transaction, by swapping option notes in such a way that neither party can interrupt the process at some stage whereby they would be able to keep both option notes. In this example, one note may be for currency, and the other note may [~~be~~] represent merchandise, such <u>as</u> a value note representation of a share certificate, currency, or [~~am~~] <u>an</u> agreement to provide certain goods or services on demand.

Please rewrite the paragraph on page 38, lines 5-13 as shown:

Another example of secure swapping or transacting value notes is described below. In this example, [~~the~~] instead of two option notes being used, only one option note is required. However, in order to redeem the option note, one party has to provide evidence that the "swap" value note has been issued, by providing the bank's signature for the "swap" value note. This example also illustrates how option notes can require signatures from other parties even though those parties may not be directly involved in the current value note transaction. The normal use of such signatures is to confirm that certain actions have taken place, e.g. between other parties, or being confirmed by another party, before the option note can be redeemed.

Please rewrite the paragraph on page 43, line 28 through page 44, line 6 as shown:

An alternative technique, illustrated in Fig. 20, is to use a short-hand notation to identify or list each value note, and to include common information, including a single instruction message, in a single message block. This is particularly suitable for value notes which have the same public key. The single message block can consist of:

(a) list of serial numbers of notes to be consolidated

(b) list of values of the notes (this is optional since the values will be known to the bank, [~~nut~~] but is preferred to reduce the chances of discrepancies after the consolidated note has been issued);

(c) single instruction message, including the basic details for the new, blank value note (i.e. new serial number (or at least the bearer's part of the serial number), public key information for the new note);

(d) bearer's signature based on (a), (b) and (c) above to secure this information.

In the Drawings:

Please amend the drawings as shown in red on the attached sheets.

In the Claims:

Please cancel claims 2 and 53-58 without prejudice.

Please amend the following claims to read as shown:

1. (Amended) A method of providing a value note comprising:

providing first information representative of a bearer's public key information [~~for a bearer~~], or from which a bearer's public key information [~~for a bearer~~] can be verified;

providing second information representative of a commodity represented by the value note; and

calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of an issuer's public key information [~~for a issuer~~].

4. (Amended) A method according to claim 3, wherein the expiry information is included in the calculation of the [~~signature~~] third information.

7. (Twice Amended) A method according to claim 5, wherein the identification information is included in the calculation of the [~~signature~~] third information.

9. (Amended) A method according to claim 8, wherein the valid-from information is included in the calculation of the [~~signature~~] third information.

13. (Amended) A method of handling a value note, comprising:

receiving a value note comprising first information either representative of a bearer's public key or from which bearer's public key can be verified, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and an issuer's public key information [~~for the issuer~~];

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the [~~payment~~] redemption instruction information and is verifiable from said first information.

15. (Twice Amended) A method according to claim 13, wherein the value note is [~~as~~] provided [~~by the method or any of claims 1 to 12~~] by:

providing first information representative of a bearer's public key information, or from which the bearer's public key information can be verified;

providing second information representative of a commodity represented by the value note; and

calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of the issuer's public key information.

18. (Twice Amended) A method according to claim 13, wherein the redemption instruction information includes a reference to transfer at least a [~~proportion~~] portion of the commodity to a first new value note.

19. (Amended) A method according to claim 18, wherein the redemption instruction information includes replacement first information for the first new value note.

21. (Twice Amended) A method according to claim 18, wherein the redemption instruction information includes a reference to transfer [~~the or~~] a remainder of the commodity to a second new value note.

25. (Twice Amended) A method according to claim 13, wherein the redemption instruction information includes an identification reference for [~~the or~~] each value note referred to in the redemption instruction information, and wherein the method comprises communicating the redemption instruction information to a value note handling authority.

28. (Amended) A method of handling redemption instruction information and bearer signature information associated with a value note, the method comprising performing at least one verification prior to redeeming the value note in accordance with the redemption instruction information, the verification comprising:

verifying that the bearer signature information matches information including at least the [~~payment~~] redemption instruction information using the bearer's public key information [~~for the bearer~~] presented in the value note or in the [~~instruction~~] redemption instruction information.

30. (Twice Amended) A method according to claim 28, [~~wherein the instruction redemption information is provided by~~] further comprising:

receiving a value note comprising first information representative of a bearer's public key or from which bearer's public key can be verified, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and the issuer's public key information [~~for the issuer~~];

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the [~~payment~~] redemption instruction information and is verifiable from said first information.

31. (Twice Amended) A method according to claim 28, wherein the redemption instruction information and the bearer signature information are received without a value note, and the method comprises retrieving value note information for one or more value notes identified in the [~~instruction~~] redemption instruction information.

32. (Twice Amended) A method according to claim 28, further comprising verifying that an issuer signature included in the value note matches information

including the [~~bearer~~] bearer's public key information and [~~the~~] a commodity represented by the value note, using an issuer's public key information [~~for the issuer~~].

35. (Twice Amended) A method according to claim 33, wherein at least one of the value note [~~and/or~~] and the redemption instruction information includes identification information for uniquely identifying the value note, and the verification comprises ascertaining whether a value note bearing the same identification information has previously been accepted.

36. (Twice Amended) A method according to claim 28, further comprising verifying whether a counter signature matches a counter signatory's public key information in the value note [~~for a counter signatory~~].

37. (Twice Amended) A method according to claim 28, further comprising verifying whether an endorsement signature in the value note matches information including a predefined message using a message endorsing signatory's public key information [~~for the message endorsing signatory~~].

38. (Twice Amended) A method according to claim 28, wherein the value note includes expiry [~~time and/or date~~] information representing at least one of a time [~~and/or~~] and a date of expiry, and the method further comprises testing the value note on the basis of the expiry information.

39. (Twice Amended) A method according to claim 28, wherein the value note includes valid-from [~~time and/or date~~] information representing at least one of a time [~~and/or~~] and a date from which the value note may validly be redeemed, and the method further comprises testing the value note on the basis of the valid-from information.

40. (Twice Amended) A method according to claim 28, further comprising redeeming the value note in accordance with the redemption instruction information, wherein the step of redeeming the value note comprises issuing a first new value note representing at least a [~~proportion~~] portion of the commodity of the value note being redeemed.

42. (Twice Amended) A method according to claim 40, wherein the step of redeeming the value note comprises issuing a second new value note representing [~~the or~~] a remainder of the commodity of the value note being redeemed.

46. (Twice Amended) A method according to claim 40, wherein at least one new value note is issued which includes information indicative of at least one of a time [~~and/or~~] and a date from which the new value note can be redeemed, and wherein the at least one of a time [~~and/or~~] and a date is later than [~~the~~] either a time [~~and/or~~] or a date [~~, respectively,~~] of issuance.

47. (Twice Amended) A method according to claim 28, further comprising communicating [~~the or~~] each [~~new~~] value note electronically to a remote party corresponding to the source of the value note being redeemed.

49. (Amended) A method wherein an electronic representation of a commodity is issued by an issuing authority, the electronic representation including information representing at least one of a time [~~and/or~~] and a date from which the electronic representation is available for redemption, said at least one of a time [~~and/or~~] and a date being later than [~~the~~] either a time [~~and/or~~] or a date of issuance, whereby the electronic representation is not available for redemption immediately after issuance.

51. (Twice Amended) A method according to claim 18, wherein the method comprises generating a first character string message, generating a second character string message from said first message in the redemption instruction information for inclusion in the first new value note.

52. (Amended) A method according to claim 51, further comprising the steps of:

communicating the value note, the redemption instruction information, and the bearer's signature information to a value note handling authority;

applying a blinding function to the second character string message to generate a blinded second character string message;

issuing [a] the first new value note including the blinded second character string message, in accordance with the redemption instruction information;

communicating the first new value note to a respondent; and

providing endorsement signature information from the respondent dependent on the first and second character string message and related to the blinding function such that the endorsement signature information is verifiable against both the first character string message and the second character string message; and

communicating the first value note [and] with the respondent's endorsement signature information to [the] a value note handling authority.

53. (Amended) A method according to claim 52, further comprising the step of unblinding the blinded second character string message by the respondent to yield the first character string message prior to providing the respondent's endorsement signature information.

61. (Amended) A value note comprising:

first information representative of a bearer's public key information [~~for a bearer~~], or from which the bearer's public key information [~~for a bearer~~] can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and the issuer's public key information [~~for the issuer~~].

62. (Amended) A record carrier on which is recorded value note information including:

first information representative of a bearer's public key information [~~for a bearer~~], or from which the bearer's public key information [~~for a bearer~~] can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and the issuer's public key information [~~for the issuer~~].

63. (Amended) A transmission signal representing a value note and comprising:

first information representative of a bearer's public key information [~~for a bearer~~], or from which the bearer's public key information [~~for a bearer~~] can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and the issuer's public key information [~~for the issuer~~].

65. (Twice Amended) A method of providing redemption instruction information for one or more value notes each being as defined in claim [~~64~~] 63, the method comprising:

providing a list of identification information for identifying each existing value note to be used in the transaction;

providing a list of redemption requests, each request including information representing a result of the transaction, and a commodity value associated with that result;

providing a bearer's signature information representing a bearer's signature which is verifiable [~~from the information in the instruction and/or from~~] at least one of the redemption instruction information and information in said value notes, and the bearer's public key information [~~for a bearer~~].

67. (Amended) A method according to claim 65, further comprising providing information representing the bearer's public key information [~~for the bearer~~].

69. (Twice Amended) A method according to claim 65, further comprising communicating the redemption instruction information, with or without the individual value notes referred to in the redemption instruction information, to a money handling authority.

73. (Amended) An electronic representation of a commodity, the representation including first [~~time and/or date~~] information representing at least one of a time [~~and/or~~] and a date up to which the electronic representation is guaranteed, and second [~~time and/or date~~] information representing at least one of a time [~~and/or~~] and a date later than either the time or the date of the first information [~~time and/or date~~] and up to which the electronic representation [~~may still be~~] is valid but without a guarantee.

74. (Twice Amended) Apparatus for carrying out a method as defined in claim 1, comprising at least one bank terminal, at least one user terminal, and a network interconnecting the at least one bank terminal and the at least one user terminal over which the value note can be communicated.